Brainwave: A Multidisciplinary Journal (ISSN: 2582-659X), Vol. 3, Special Issue, March 2022, pp. 31-34 © Brainware University

Cloud Computing An Unsung Hero Of Covid-19

Shreya
Computer Science & Engineering
Brainware University, Kolkata, India
singhshreya747392@gmail.com

Abstract

Taking into account the COVID-19 outbreak unfolded by the novel coronavirus, every organisation instructed their workers to work from home as a preventive measure to reduce the danger of infection and contagion. However, in order to make contact, discuss and collaborate in the virtual space securely, the world needed an advanced infrastructure for a smooth digital transformation. This challenge was taken up by cloud computing and emerged as an unsung hero in the widespread disaster.

Cloud computing comprises the speedy execution for services that depicts the rapid use of flexible applications for maintaining data. But in spite of a huge surge in the utilization of cloud computing applications, there exists a continuous research challenge in the area of cloud computing environment regarding information, promising safety and the accessibility of CC applications. The rapid acceleration in volume of data generation post global spread of virus is another aspect of this rising challenge. When exigent questions arise, an answer is essential. This paper, to the best of my knowledge, thoroughly explains how this technology has helped control this infection to save millions of lives worldwide, the influence of the COVID-19 pandemic on CCE and points out the security risks of working virtually from home.

Keywords:
Cloud computing,COVID-19,Big data privacy,Security,Pandemic,Coronavirus,Digital transformation.

Introduction

Coronavirus disease 2019 (COVID-2019), formerly termed as 2019-nCoV, has brought disorder globally. It first turned up in December 2019, with an article declaring how people were suffering from breathing problems and fever after their shopping in a seafood mart in Wuhan, Hubei, China. In not more than a month, the infection of 2019-nCoV spread to every corner of the world be it Thailand, Vietnam, Japan, Singapore, Germany, America, India etc [1]. Till now over 120 countries' citizens have been infected [2]. Due to this rising number of affected humans and deaths each day, most nations in the world began taking this outburst seriously. Many of them commenced their investigations into the unfolding of the ailment by monitoring contact and collecting epidemiological and clinical data from patients to find treatments [3].

On the other hand, the showcased cases were isolated and strict hygiene practices were adopted. Furthermore, administrative authorities announced strict lockdowns across their nations to limit the possibility of spreading the disorder. Schools and colleges in twenty-nine nations have been closed, affecting 391 million children and youngsters. Similar measures are being taken for faculty, staff, and workers in firms throughout the world are it Google, Microsoft, Cisco, Tesla, Facebook or Twitter [4].

Approximately every sector, including small and large groups, healthcare, and training, have been compelled to electronically convert their offerings. Because of these measures, the consumption or need for cloud service providers (CSPs) has been rapidly growing. Thereby, promising a hard set of

challenges for CSPs to face in order to offer first-class quality services constantly, handling an explosive boom of demand because of coronavirus.

The need for cloud computing services (CCS) has increased the speed, volume, and quality in statistics being generated each second around the world from various services and applications [5]. The generated data could be in the form of structured, semi-structured, or unstructured data. This collected data is stored in various formats with a large data flow of non-integrated data at high speeds [6].

Thus, this paper explores the following questions:

a) How has the pandemic upsurge affected CCE?

b) What are the troubles that could arise in a virtual environment from a security perspective?

Influence of pandemic on cce

Indeed, even in this COVID-19 pandemic, the association with CCE might be an ongoing relationship, except if a fresh out of the blue new innovation comes. CCE is a framework constructed from applications, IT foundations, and organizational administrations. It utilizes the assets of a data community, which might be shared through the virtualization innovation. This utilization of administration is flexible, instant administrations and rates. They are furthermore charged as a service bill [7,8].CCE attributes might be imagined in an exceptionally graphical form. With this thought of "figuring as a utility", there is as much potential in CCE as that in gas, power and water. With choices like 'sitting and playing', or possibly a "pay more only as costs arise" framework, the potential is huge. Clients have the liberty to choose their software, stage and infrastructure needs. Having this capability, clients need not to plan for IT development inside the near future. As an adequacy, there's feasibility and quick access. Notwithstanding, similar to each figuring highlight, there will be security gaps in risks and dangers [9].

CCE needs extra addition in the sphere of safety to lessen or close these holes. The cloud model consists of two sections:

a) CSP that conveys cloud administrations and

b)Cloud users who are represented in the organizations who have access to the provided cloud services. Other various components are the cloud auditor and the cloud broker. The rapid increment of new applications throughout the Internet, has also increased the need for better security [10].

The hardware, software, and infrastructure as a service is now a whole set of aspects that are included in the CC model. These prototype models are now categorized under a branch of service offered.

This includes three classifications namely;

Infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

There are four models in cloud deployment:

a)hybrid cloud b) public cloud c) community cloud and d)Private cloud [11,12].

Every model states wherefore the cloud is actually deployed and whatever is available to customers. The virtualization technology is used to establish CCE. This virtualization is a hypothetical complexion called the virtual machine monitor (VMM). It can also be called a hypervisor layer sandwiched in the hardware, operating system and applications. VMM is somehow similar to a controller that controls the hardware resources which enables multi-engagement. For sharing

resources, multi-engagement allows multiple operating systems to reside over the same physical hardware at the same time [13].

Safety issues of domestic virtual work space

Many sorts of enterprise models are there in the market, including business-to-consumer (B2C), business-to-business (B2B), and business-to-government (B2G). These styles of business models have not been often in call for in many nations until online consumer groups have become dense, high in demand and closely saturated. But recently, COVID-19 situation has all of a sudden regenerated domestic-to-X terminology, like home-to-business (H2B), home-to-government (H2G), or home-to-consumer (H2C). This era involves digital conferences, virtual healthcare, online training,cybersecurity, logistics to advanced cities, faster streaming and many more [14]. This "stay-at-home" scenario to restrict the spread of this ailment isn't for a short duration, and might expand over months and years. Therefore, shifting work home is vital for keeping the continuity of professional jobs.

However, conversely, this will result in unforeseen danger in security issues. These issues can be broadly divided into four categories;

a) Internet
b) Data privacy
c) Personal devices
d) Applications
e) CCE

Limitations of the research

There exists a lack of proper resources that could clearly illustrate the attack cases which took place on CCE in this period because the crisis is ongoing.

Conclusion

The reliance on CC applications has drastically accelerated because of the modern-day scenario of the COVID-19 pandemic. No doubt, this catastrophe has impacted nearly all sectors, including tourism, healthcare, education etc. The speedy unfolding of COVID-19 has also elevated the volume of facts generated from diverse resources. This boom of information demands novel technologies, additional data storage systems etc. which creates a crucial task.

In this paper, I've tried to show the impacts of the COVID-19 crisis on CCE. Besides this, the paper analyzes the safety risks for virtual working space. From a security perspective, the modern-day state of affairs may divulge each CCE and its users to exceptional varieties of assaults because of the lack of preparedness to stand one of these unlooked situations [15].

Users are probably prone to one-of-a-kind kinds of attacks as they perform untrustworthy Internet programs on their own domestic devices, which won't be updated with the ultra-modern safety regulations. Therefore, at-home workers might grow to be the target of attackers without problems stealing massive amounts of information. Therefore, making it essential to deal with the safety dangers that CCE and customers face, as well as to upwardly push the notice the threats of the usage of unsecured devices to get entry to the Internet whilst they may be operating from domestic zones.

References

[1] https://plus.google.com/+UNESCO. (2020, March 4). Education: From disruption to recovery. Retrieved February 7, 2022, from UNESCO website: https://en.unesco.org/covid19/educationresponse

[2] British Broadcasting Corporation, Coronavirus: School closures and travel curbs in UK plans. Available, https://www.simhospital73.com/2020/03/coronavirus-school-closures-and-travel.html, April 2020.

[3] Office of Postsecondary Education, Guidance for interruptions of study related to coronavirus (COVID-19). Available, https://www.eou.edu/coronavirus/files/2020/03/COVID_19-EA-Guidance-for-interruptions-of-study-related-to-Coronavirus-COVID-19.pdf, April 2020.

[4] Alashhab, Z. R., Anbar, M., Singh, M. M., Leau, Y. B., Al-Sai, Z. A., & Abu Alhayja'a, S. (2021). Impact of coronavirus pandemic crisis on technologies and cloud computing applications. Journal of Electronic Science and Technology, 19(1), 100059.

[5] Z.A. Al-Sai, R. Abdullah, M.H. Husin(2019). Big data impacts, and challenges: a review. *Proc. of IEEE Jordan Intl. Joint Conf. on Electrical Engineering and Information Technology*, pp. 150–155.

[6] R. Krishnamurthi, M. Goyal(2019). Enabling technologies for IoT: issues, challenges, and opportunities, in: B.B. Gupta (Ed.), Handbook of Research on Cloud Computing and Big Data Applications in IoT, IGI Global, (pp. 32–82).Hershey.

[7] D.S. Linthicum (2009). *Cloud Computing and SOA Convergence in Your Enterprise: A Step-by-step Guide*, *Addison*, Pergamon: Wesley Professional.

[8] A. Amairah, B.N. Al-Tamimi, M. Anbar, K. Aloufi.(2019). Cloud computing and internet of things integration systems: a review, In F. Saeed, N. Gazem, F. Mohammed, A.Busalim (Eds.), *Recent Trends in Data Science and Soft Computing*(pp. 406–414), Springer.

[9]J.W. Huang, D.M. Nicol. (2013) Trust mechanisms for cloud computing, *J. Cloud Comput.: Adv. Syst. Appl. 2* (1), 9,1-14.

[10] P. Mell, T. Grance. (2011). The NIST Definition of Cloud Computing, *National Institute of Standards and Technology*.

[11] S.H. Na, J.Y. Park, E.N. Huh. (2010). Personal cloud computing security framework, In *Proc. of IEEE Asia-Pacific Services Computing Conf*,(pp. 671–675). Hangzhou.

[12] S.T. Alanazi, M. Anbar, S. Karuppayah, A.K. Al-Ani, Y.K. Sanjalawe. (2019). Detection techniques for DDoS attacks in cloud environment: review paper, In V. Piuri, V.E. Balas, S. Borah, S.S.S. Ahmad (Eds.), *Intelligent and Interactive Computing* (pp. 337–354). Singapore: Springer.

[13] Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, M. and Leaf, D. (2011). *NIST Cloud Computing Reference Architecture, Special Publication (NIST SP*), National Institute of Standards and Technology, Gaithersburg.

[14] Liao, Rita. (2021, 21st August). China Roundup: enterprise tech gets a lasting boost from coronavirus outbreak

TechCrunch. Retrieved from

https://au.news.yahoo.com/china-roundupenterprise-tech-gets-211510312.html, April 2020.

[15] Stergiou, C.L., Psannis, K.E., Gupta, B.B., & Ishibashi, Y. (2018). Security, privacy & efficiency of sustainable Cloud Computing for Big Data & IoT. Sustain. Comput. Informatics Syst., 19, 174-184.